

属性証明の課題整理に関する有識者会議(第1回) 議事録

○日時

令和7年10月23日(木)10:00~12:00

○出席者(敬称略)

(委員)

板倉陽一郎 (ひかり総合法律事務所 パートナー弁護士)
笠井玲子 (株式会社ローソン インキュベーションカンパニーデジタルソリューション推進部 シニアマネジャー)
國領二郎 (慶應義塾大学 名誉教授)
崎村夏彦 (NAT コンサルティング合同会社 代表社員)
瀧俊雄 (株式会社マネーフォワード 執行役員グループ CoPA マネーフォワード総合研究所長)
中村素典 (京都大学 情報環境機構 IT 基盤センター長・教授)
富士榮尚寛 (OpenID ファウンデーション・ジャパン代表理事)
松尾真一郎 (ジョージタウン大学研究教授およびバージニア工科大学研究教授)
松本泰 (特定非営利活動法人 日本ネットワークセキュリティ協会フェロー)
横田明美 (明治大学 法学部 専任教授)

(デジタル庁:事務局)

楠正憲 (デジタル社会共通機能グループ長)
その他関係者

○欠席者(敬称略)

若江雅子 (朝日新聞東京本社 編集委員)

○議事

(デジタル庁北井上)

ただ今より属性証明の課題整理に関する有識者会議第1回を開始いたします。皆様、本日はお忙しいところ、お時間をいただきまして誠にありがとうございます。私は事務局を務めますデジタル庁の北井上と申します。よろしくお願いたします。早速ではございますが、本会議の開催に当たり、事務局を代表して、デジタル庁デジタル社会共通機能グループ参事官の中川より一言ご挨拶申し上げます。

(デジタル庁中川)

デジタル庁の参事官をしております中川と申します。本日は國領先生を始め、構成員の皆さんにお集まりいただきましてありがとうございます。開催に当たりまして、一言事務局を代表させていただきますましてご挨拶させていただきますたいと思います。

昨年度も含めて大変お世話になりました、昨年度違う名前でごございましたね。「DIW アドバイザリーボード」と、「Verifiable Credential (VC/VDC) の活用におけるガバナンスに関する有識者会議」ということで、いわゆる VC・DIW の利活用促進に向けてご議論を賜ったと思っています。今年度、名前は変わりましたが、その趣旨としまして、いわゆる VC・DIW をツールではなく目的ということで、デジタル庁の中でも「ミッション・ビジョン・バリュー」があるのですが、バリューの中で「常に目的を問いかけ」という言葉がありまして、この目的って何だろうと考えたとき、それにふさわしい名前で広く社会に向かって打ち出していくという意味でも、デジタルにおける属性証明という形で少し広く捉えさせていただいた形でございます。それによって行政手続のデジタル完結であるとか、データ利活用の将来像、このような、もう少し広めの議論をさせていただく場としてできればなという思いがございます。こうした意味で、今回の会議名である「属性証明の課題整理に関する有識者会議」という名称に変えて、立ち上げさせていただいたという趣旨でございます。そういう意味では、国内でも EU でも教育クレデンシャルみたいなことで動きが検討されていますけれども、属性証明の電子化や高度化、これらがますます高まっているという状況でございます。特に日本ではご議論いただいたところもあるかと思っておりますけど、住民票の写し、これを電子交付しますというところの Verifiable Credential、VC、これを記載されているというふうな意味で具体的なことだと思います。

昨年度の会議でも、この時にリスクとして生じるのが、紙の証明書ではなかった名寄せということで、基本的にはそれだけで完結せず、誰かが名寄せしてしまって、いろんな情報が一緒になってしまうというリスクも生じるのではないかとということをご指摘いただいたかと思っております。どのような対策を講じることでリスクを減らせるのか、というようなところが議論の対象になるのではないかと思います。技術的に対応できるということもあるでしょうが、法制度的に何かしらの手段でやらなければいけないということもあるかもしれません。こういう風な手法がどうあるべきか、というところをご議論賜れるとありがたいと思っております。そういう意味で、広くご議論いただければと思います。過去には、こういう技術もあるとか、こういう手法もあるのではないかとということで、特にいろんな手段があちらこちらに議論がいくこともあったかもしれませんが、この目的を常に問いながらご議論いただければありがたいと思います。長くなりましたが、私からは以上でございます。よろしくお願い致します。

(デジタル庁北井上)

続きまして、本会議の進め方についてご説明いたします。資料 1 の設置要項をご覧くださいと思います。傍聴の皆様、ホームページの公表資料ではなく、現在投影している資料の方をご覧くださいと思います。

それでは冒頭から説明をさせていただきます。本会議は、行政手続等のデジタル完結や自動

化等に必要な属性証明の実現をしたいと、こういった我々の大目的に向けて VC・DIW の利活用を進めていきたいと考えております。一方、新しい技術であるがゆえに想定されるリスクですとか、リスクに対する適切な技術面・運用面の対策などが整理されていないと、こういった状況がございます。このため、本会議ではこれらの対策の実施を促す手法等についてご議論いただきたいと、このように考えているところです。委員は3にありますが、ご覧の11名ということでございます。お一人お一人のご紹介というところは、時間の都合上割愛をさせていただければと考えております。

次のページをご覧ください。座長は委員の互選により決定、事務局はデジタル庁となります。続きまして6のワーキンググループのところでございます。特定の議題について詳細な検討を行うために、ワーキンググループを設置する旨の規定がございます。資料3というところをご覧くださいと思います。後ほど詳細を説明いたしますけれども、こちらに記載のとおり本会議については技術にかかる議論というところが、一定想定されるところでございますので、技術ワーキンググループというものを置く予定でございます。具体的な予定等については、事務連絡として最後に改めしてお伝えいたしますので、この場では省略いたします。

資料1に戻ります。7に記載のとおり、要すればゲストスピーカーおよびオブザーバーを求めることが可能ということになっております。

最後に本会議は原則現状のとおり公開ということにさせていただき、資料や議事録なども公開をさせていただくということで考えております。説明は以上となります。

本会議の進め方についてご質問・ご意見がございましたら挙手を、あるいはオンライン参加の委員におかれましては、機能の挙手ボタンというものを押していただければと思います。

<質問・意見なし>

特段なさそうですので、こちらのとおり本会議進めさせていただきます。それでは続きまして、設置要項に従いまして、委員の互選により本会議の座長を決定させていただきたいと思っております。事務局としては、昨年度の「DIW アドバイザリーボード」に引き続き國領先生をご推薦したいと、このように考えてございますが、どうかご異議がある方は挙手を、オンライン参加の委員におかれましては挙手ボタンを押していただければと思います。

<異議なし>

ご異議ございませんでしたので、本会議の座長を國領先生にお願いしたいと思います。國領先生一言ご挨拶いただけますでしょうか。

(國領座長)

おはようございます。昨年に引き続き、名前が変わりましたが、この会を取りまとめさせていただくこと、大変光栄に思っております。だいふ機が熟してきたような気がしております、具体

的な道筋が少しでも見えてくればいいなと思っておりますので、委員の皆様と事務局の皆さんのご努力をぜひよろしくお願い申し上げます。どうもありがとうございます。

(デジタル庁北井上)

國領座長ありがとうございます。それでは次の議題に移りますが、議論に入る前に事務局から会議の設置目的や今年度のゴール感、議論のスコープ、リスクや対策といった点につきまして、あらかじめ資料の説明をさせていただければと考えております。資料を説明した後に議論に関する進行という部分につきましては、國領座長にお願いできればと考えておりますので、よろしくお願いいたします。それでは事務局から資料 2 に基づいて、それぞれ説明をさせていただきます。

(デジタル庁中川)

資料 2 をご説明します。最初の方、私の方でご説明をさせていただきまして、後ほど交代をさせていただきながら、詳しくご説明させていただきたいと思っております。

まず趣旨・目的ということになりますけれども、背景課題は既にご案内のことかと思っておりますけれども、ある程度具体的にアウトプット出していけないといけないところだと思っておりますので、改めて趣旨・背景・課題というところをご説明させていただけたらと思っております。

私もちょうど先週病院に行ってきましたけれども、マイナンバーカードで保険診療もできるようになっていて、スマートフォンでももうできるようになったというレベルぐらいで、身元証明書であるとか、保険の証明みたいなものはデジタル化が実現したのであろうと思っております。ただ、住民票の写しや、入学・入社の際に必要な成績証明・在学証明、これは公的機関が発行するだけでなく、民の中で証明される証明書というものもありまして、これについてはデジタル化が未了であるということが多く思っています。これをうまくやらないといけない、そういう意味では本丸なのであろうということです。PDF でこういう現在の証明書というのは発行されることもありますけれども、やはり改善点やご指摘があったところだと思っておりますが、この 2 点、主にあるのかなと思ってございます。こういうところを乗り越えて、資格証明や属性証明ということをやって、電子化や高度化をやっていくことが必要だと思っております。

その意味でこの会議の趣旨・目的ということになりますが、各種の証明書の電子化・高度化をするにあたって、やはり民間企業の皆さんにサービスとして広まっていくということも重要であろうところだと思っております。先ほど申し上げた成績証明のようなもの、各高校、私立高校とか公立高校も含めてですけれども、これを導入していこうとなると、安価であり、簡便であり、迅速に実施できるということが重要だと思っております。この辺、技術オリエンテッドでやってしまうと、安全だけれども高いものになってしまったり、導入するのに時間がかかったりといったことになると、なかなか広がらないということになってくるかと思っております。制度の面でも、法律を作るとか罰則もできるみたいなことは、相当ハードルが高くなる。また、手続が必要なことがあるとか、またさらにハードルが高くなってしまいうところもありますから、制度的な部分のコストというの、なるべく最低限にしないといけないだろうと思っております。この点が本当にポイントなのだろうと思っております。

なるべく安く簡単に、そして迅速に、ここを忘れないようにしながら、議論をやっていくということが必要なのかなと思っています。紙と比べて便利なところ、安全であるところも問いながら、検討を進めていただくと、大変ありがたいかなと思っています。また、こういった証明書一般について、制度的側面からもアドバイスを賜れば、ありがたいと思っています。

次のページから基礎情報になります。Verifiable Credential、VC とはどのようなものであるのかであるとか、DIW がどのようなものであるのかということが書いてあります。これは改めてとはなりませんけれども、今回初めて傍聴にもお越しいただくような方もいらっしゃると思いますので、こちらでも記載させていただいてございます。

次のページが「証明書の電子化及び高度化に向けて取り組むべきこと」でして、一番左が今のマイナンバー、マイナンバーカードで実現できているというところではあるかと思います。身元証明書に相当します。中央の列が資格確認、右の列が民間の発行する属性証明書です。資格証明書、属性証明書、これらについては、この会議のスコープになる、要対応と書かせていただいているところです。それぞれ、未整理であるところ、またこういう規定をする必要があるのかなというところを、まとめて書かせていただいているというところがございます。私の説明は以上になりますが、この後の「はじめに」というところまで事務局からの説明を続けさせていただければと思います。

(デジタル庁澤田)

それでは以降はデジタル庁の澤田から説明させていただきます。まず、昨年度の議論の振り返り、そして直近の動向の紹介をさせていただきます。

昨年度の「DIW アドバイザリーボード」では、DIW には各ステークホルダーにさまざまなメリットがあることを整理いたしました。DIW の活用が期待できるユースケースの類型を整理いたしました。そして、それら VC や DIW を活用する際に懸念されるリスクについても洗い出しました。リスクへの対策、ガバナンスとしてどのようなことが必要かについて、Verifier あるいは Wallet Provider に対してどのようなガバナンスが必要かというご意見を頂戴しました。もう1つの会議体である「Verifiable Credential (VC/VDC) の活用におけるガバナンスに関する有識者会議」では、特に Issuer が担うべき責任や Issuer が留意すべき点について議論をいたしました。これらの議論を踏まえまして、「DIW アドバイザリーボード」の報告書では、各種のリスクに対し既存のガバナンスで既に対策が講じられている点も考慮の上で、VC や DIW 固有で必要な対策について、技術・運用・制度の面の論点があると、このようなフレームワークを整理するまでまとめました。今年度はこの議論の継続ととらえていただけたらと思います。また、併せて今後の将来展望についても、VC・DIW により便利で効率的なデータ連携を進めることができ、それらを安心して利活用できる、また新たなサービスなどの価値が創出される、このような展望を整理したところです。以上が昨年度の議論の簡単な振り返りとなります。

続きまして、直近の VC 活用への期待の高まりとして、2 つの例をご紹介します。まず、行政側での期待について、今年度、総務省でのワーキンググループにおいて、住民票の発行や電子化についての検討がされているところです。オンラインの申請という意味ではなく、電子

媒体での発行に関するものです。こちらに関して、PDF ではなく等身等のリスクが懸念されるところ、VC の活用の可能性を含めて検討が進められているところです。また、民間においても、新しい技術やビジネスと併せて使う可能性の期待がございまして、先月発表された新しいプロトコルでは、AI のエージェントがユーザーの委任を受けて何らかの購入決済等の処理を行う時に、その委任を正当に受けていると示す VC を発行して活用するとのアイデアが発表されています。このように VC や DIW に関する関心や期待はますます高まっていると認識しております。以上が議論の前提となるご紹介でした。続いて、このまま論点のご説明に入ります。少々説明が長くなりますが、通して説明させていただきます。

まず、今年度の本会議で取り扱う論点について明確化をさせていただきます。本日開催の本体会議では、VC・DIW による証明書の電子化・高度化におけるリスク対策について、適切な技術面・運用面の対策をどのように示し、実施を促すべきかを議論いたします。この点について、先ほど紹介しました昨年度のまとめでは、「技術・運用・制度」というフレーズを使っておりましたが、冒頭、中川から申し上げたとおり、制度によらずとも技術・運用の対策は可能な場合がある、ということで、資料中の青字のとおり「適切な技術面・運用面の対策を促す手法」という表現をさせていただいております。また、今後開催していきます技術ワーキンググループでは、技術・運用面の対策について、推奨する具体の技術要件を定義し、本体会議にフィードバックしていきます。ここで議論の前提として、1 点ハイライトしておきたいのが、上の本体会議の記載になりますが、今回は「公的かつリスクの高いユースケース」に必要な対策は何か、として考えていただきたいという点でございます。

公的なユースケースとは何か、について、委員への配布資料のみにイメージ例を列挙したものを示しております。委員の皆様はお手元の資料をご覧ください。公的なユースケースは、公的機関が発行する各種証明書、あるいは逆に民間が発行し行政機関が受けとるもの、両方含めて公的なユースケースとしております。また、公的かつリスクの高いユースケースとは何かにつきましては、具体例がないと議論しにくいと思いますが、例えば先に紹介した住民票の写しを仮に VC 化した場合などが該当すると考えております。行政機関が発行し、氏名や住所などの個人情報が含まれる証明書であり、かつ提出場面が多いもので発生するリスクがある証明書、これが公的かつリスクの高いユースケースと捉えてご議論いただければと思います。

次に講じるべき対策の前提となる、懸念されるリスクと、脅威についてご説明をいたします。こちらは昨年度の議論でのリスク整理を踏まえ、VC のライフサイクルに沿って脅威を整理し直したものといたします。各種 VC や DIW の活用に関してのリスクと脅威がございまして、こちらの脅威についてリスクの類型をまとめて示したものがこちらでございまして、1 つ目が「正規の VC の盗用や再利用に詐称・なりすまし」、2 つ目が「偽造 VC や派生 VC の受け入れ被害」、3 つ目が「VC に起因するプライバシーの侵害」、4 つ目が「VC の可用性や利便性の低下」でございまして、こちらの 4 つのリスクの詳細はこの後説明いたします。なお、補足ですが、今年度の議論において、必ずしも全ての VC・DIW のリスクを網羅できるわけではなく、Web サービスの一般に起因するリスクや、対策の内容や促進に関しての論点が少ないようなリスクは、議論から捨象させていただいております。

それでは次に、この4つのリスクに関して、それぞれリスクの詳細及びそのリスクの対策の概要を説明していきます。

まず、1つ目のリスクの「正規の VC の盗用や再利用による詐称・なりすまし」についてです。これは VC のライフサイクルのさまざまな場面で、攻撃によって VC の情報が盗まれる、漏洩するなどした時に第三者が VC を悪用してしまう、このリスク全般のことです。次に、このリスクに対する、主な対策としては大きく分けて 2 つあると考えられます。中段に記載のとおり、1 つ目が Holder の署名鍵や本人確認情報などの Holder を特定する情報を VC に紐付ける、「Holder Binding」と呼ばれる対策です。2 つ目が Wallet 内でのデータの扱いについて、不正アクセスや複製を防止する対策を強化する、などです。これらの対策の具体的な手法やその使い分けは技術ワーキンググループでの論点となります。この本体会議としましては、このような詐称・なりすましの対策のために、どのような場合に、どこまで「Holder Binding」などの対策の実施を Wallet Provider に促し求めていくのかという視点で、この後ご議論をいただきたく思います。

次に 2 つ目のリスクとして「偽造 VC や派生 VC の受け入れ被害」についてです。VC はその性質上、発行以降の改ざんは署名の検証等で検知ができますが、発行時点で行われた行為は検知できません。そこで、悪意のある偽の Issuer が偽造 VC を発行するリスクというものが、まずあります。もう 1 つご紹介しております派生 VC というのは、「原本となる証明書をもとに発行された別の証明書」のことですが、特に原本発行者ではないものが原本の信頼性に基ついた派生 VC、これを発行してしまうという不適切な運用がありますと、原本の証明書が失効・変更されても、それが反映されないといった情報の正確性などの課題がございます。このような発行時点で発生するリスクに対する対策としては、VC の発行元が適切な主体か、これを Issuer の適格性と呼びますが、これを検証する必要があります。特に多数の Issuer がいるユースケースでは、この対策が期待される場合があります。具体的な方法としましては、資料の右下の図のように、第三者機関が Issuer を審査・登録したリストを公開しまして、それを Verifier が参照、検証できる仕組みが想定されます。この Issuer の適格性検証に関しては、何を適格性として検証するのか、といったことがこの本体会議での論点となります。左側に示しておりますとおり、例えば、行政機関発行の証明書であれば、それが実際の行政機関であるのかということを通格性として検証することも考えられます。民間の発行につきましては、すべての企業の適格性の検証、これは困難だと思いますが、例えば医療、金融のような、公共性が高く、すでに認可のされた事業者のリストがあるような分野であれば、リスト検証も可能かもしれません。EU や米国でも、このような Issuer の適格性の検証の仕組みは、すでに提供されているところです。踏まえて、どの範囲でどの程度このような対策が必要かについて、ご検討いただきたく思います。

3 つ目のリスクとしては、「VC に起因するプライバシーの侵害」でございます。VC には署名値などの名寄せがしやすい情報が含まれるところ、複数の Verifier が提示を受けた VC の情報を意図的に共有し合ってしまうと、選択的開示によって守られたはずのプライバシーが侵害されてしまうリスクがあるというものでございます。このリスクに対する対策としては、大きく分けて 2 つの対策があります。1 つ目が、複数の情報を提示した主体が同一であると紐付けできないようにする、

Unlinkability と呼ばれるものであります。これを技術的に実現する手法については、様々ございまして、その使い分けについては特に技術ワーキンググループでの議題とさせていただきます。2 つ目の対策が、そもそも VC を提示する相手先を信頼できる相手に制限してしまうというものです。しかし、アナログの証明書でも、制度的に提示先を制限しているものは、身元証明以外にはほぼないところ、過剰な対策とならないように留意する必要がございます。本日はこのプライバシーの対策については、どの手段をどこまで求めるべきかという観点でご意見をいただきたいと思っております。

最後に 4 つ目のリスク、「VC の可用性や利便性の低下」に関してです。こちらは Wallet Provider や Issuer がサービスを終了、あるいは端末を交換した際などに VC に必要な互換性がない場合に、VC が移行できず使えなくなってしまうといったリスク全般のこととございます。このリスクへの対策としましては、Wallet Provider に対しては、一般に民間企業に事業終了時の対策を求めるというのはハードルが高いところ、例えばですが、VC の相互互換性について推奨要件としていく、などが考えられるところです。また、Issuer に対しては Issuer が VC の発行サービスを終了してしまった後も、発行済みの VC の証明能力を損なわない対策をガイドラインで示していくなどが考えられるところです。本体会議としましては、このような Wallet Provider と Issuer が備えるべき要件を、どこまでどのように示していく必要があるのか、こちらを論点とさせていただきたいというところです。なお、欧州や米国ではこれらの相互互換性への手当は一定なされているところとして、欧州の一部の国のように、政府自身が Wallet を提供するといったような場合は、Wallet Provider の撤退リスクは考慮しなくても良いということになります。

以上が 4 つの VC・DIW 固有のリスクと、考えられる対策の概要でございます。最後に、次のページ、机上配布のみとしておりますので、お手元ご覧いただきたいのですが、リスクの一部は既存の法令の対象にもなり得ると考えられますところ、関連法令についてお手元で示しております。事務局からは、この場でこの各法令の適用範囲の整理や見解を示すことができかねますが、既存のガバナンスでカバーされているのかといった点も踏まえてご意見をいただきたいと思っております。ここまでが議論の前提となるリスク、また、実施促進のあり方を議論したいリスク対策の説明でございます。事務局からの資料説明は以上となります。それでは改めまして、以降の議論の進行を國領座長にお渡ししたいと思います。

(國領座長)

この後で、この会のゴールをどういうゴールにするべきかといった説明と、事務局からのご提案と議論がある予定になってはいますが、それがまた後から来るということを前提としながら、ここまでの資料につきまして、何か質問とかご意見とかいうのがありましたら、募りたいと思うのですけれども、いかがでしょうか？

(富士榮委員)

改めまして OpenID ファウンデーション・ジャパンの富士榮でございます。今年もよろしくお願いたします。前半入れていなかったこともあるので、もしそういうご説明あったら重複してしまうかも

しれないですけども、今の澤田さんのご説明をお伺いして感じたことなのですが、全体の議論を少しミスリードしないようにされた方が良かなというふうに感じているところがありまして、全体的にリスクの話にフォーカスをし過ぎてしまっているのではないかなというふうに感じています。何を言いたいかと言いますと、リスクがあるケースというのは、もちろん Verifiable Credential を含めたデジタルクレデンシャルの用途並びに性質によっては、あるとは思ってはいるのですけれども、リスクのないケースというものを逆に洗い出して、そこから社会実装を進めていくという道も考えないと、これは全体的に危ないものだという意識が付きすぎてしまうのではないかな、というようなミスリードを生むのではないかと感じた部分がございます。

例えば具体的に言いますと、Holder Binding の話がございましたが、本当にすべてのクレデンシャルにおいて、Holder Binding をしなければならないのかということ、バインドの強度がそれほど強くなくても機能するような資格証明の話とかはあると思うので、そういうところをまず腑分けするところから始めても良いと思います。派生クレデンシャルの話に関しても、例えば Apple が US で始めましたけれども、ID in Wallet の話とか、いわゆる派生クレデンシャルとして社会実装がされている部分もあると思います。全体的に言えるのですが、すべてを実印として扱うみたいな運用ってありえないと思うので、派生でも良いよというケースというのは、Verifier の側の判断としてはあり得ると思うので、であれば派生であるということ Verifier がわかるという前提において、派生でもいいぞっていうケースを少し具体的に出してあげるというのも、逆にガチガチに縛るよりも良いケースもあるのだらうと思います。端末交換を含めた、いろんな鍵の管理の問題もありますけれども、先ほどご説明にもありましたが、いろんなところでいろんな取り組みされております。例えばドイツなんかは、クラウド HSM を使うみたいなのところも、実際に運用として乗ってきていると思うので、そういうワークアラウンドと言いますか、選択肢というものをちゃんと提示をしていくことによって、縛る方向ばかりじゃないような議論にしていけると良いのではないかなというふうに思いました。一旦以上です。

(國領座長)

ありがとうございます。ユースケースの絞り込みについて、具体的なイメージを持って、富士榮委員が今おっしゃっていただいたのは、実現ができる可能性が高いような、リスクが低いものから具体的に考えて実装するようなことを考えると良いのではないかなというご意見だったと思います。その観点から考えて、今この資料の中では例示として、住民票の例と AI エージェントの例とかが出ているわけなのですが、こういった考え方で話を進めていって良いのか、何でしたら別のユースケースを「想定すべきユースケース」みたいなものとして考えた方がいいと思っていられるのか、その辺もしご意見あったらお願いします。

(富士榮委員)

ありがとうございます。そうですね、ユースケースとして住民票と AI エージェントの話がありますが、例えば AI エージェントのケースも、マニフェストを使ってという実装の内容とか、プロトコルの

内容について理解はしているのですけれども、国発行のクレデンシャルを使うのか、みたいな話とかも含めて、もう少し緩いケースがもう 1 つぐらい作れないかなというのは思ったところではあります。

(國領座長)

ありがとうございました。松本委員どうぞ。

(松本委員)

リスクの話から入るのがいいのかなっていうのは、やっぱり疑問を感じました。利便性であるとかメリットを理解した上で、リスクを見るのが本当はいいのではないかと思いますよね。ただ、今アーキテクチャがそもそも確定しているわけじゃないので、リスク分析は難しいと思うけども、今の話を聞いていて、私が去年も一昨年も付き合っているんで、それで理解できるのだけども、今の話を理解できる人はほとんどいないのではないかと思います。リスク分析としてやれるといいなと思ったのは、明確にすると良いなと思ったのは、誰にとってのリスクなのかというのが、よくわからなかった。わからないというか、ここには明記されていない。大きく分けたら本人と Relying Party、Verifier がありますよね。その分類は最初にあると本当はわかりやすいのではないかと思います。もう 1 つは、攻撃者が誰か、攻撃者は悪意ある第三者みたいな話とか、悪意というか、コンプライアンスがない Relying Party、Verifier 色々あると思うのだけれども、そういった分類で分類するのが良いと思ったのだけれども、紙の証明書の場合、社会的に問題になるのは、間違いなく本人が攻撃者なのですよね。偽造したのが本人だから。そういった観点の分類があるとわかりやすいのかなと。VC ははっきりいって難しいですから、それを前提にリスク分析しても、わかる人はわかる、わからない人はわからないと思いました。

少し気になったのが用語の使い方で、これも細かい話もしようがないのだけど、スライド 30 に「適格な Issuer」、「適格な VC」という言葉があるけれども、3 つありますと、実際の Issuer であるとか、派生の VC とか。ヨーロッパの eIDAS2.0 では、「適格な Issuer」というのが、Qualified Issuer と言うのですよね。Qualified Issuer があって、さらに言えば軽い用途では、Non-Qualified があるのです。だから Issuer にも 2 つの保証レベルがある。ここの中で全く議論がない、必要あるかないかは別にして、LoA (Levels of Assurance) みたいな、そもそも VC って一つの保証レベルだけなのという議論が必要では？ そこも含めて「適格な Issuer」と書いてしまうと、これはヨーロッパの Qualified Issuer のことを言っているのか、と思う人もいる。これは日本語、Qualified を日本語でどう訳すかとか、そういった問題も確かにあって、そこは注意しないとイケないのではないのでしょうか。

(國領座長)

ありがとうございます。ほかにご発言を要求されている方はいらっしゃいますか。

(笠井委員)

ローソンの笠井と申します。よろしくお願いいたします。事務局説明資料の 17 ページ、18 ページのところ教えていただきたいのですけれども、住民票の発行の写しのところは、私どもコンビニの方でのコピー機の発券というところで実施しているケースが多いのかなと思っております。今回、これを VC にというお話ですが、利用後のシーンというか、私たち VC をできましたと言って、どうやって提出をするというところが、この 17 ページも 18 ページも全てオンラインなのか、それとも間で対面のどこかに行き、提出をするみたいなことなのか、というところのフォーカスとしては、この両方を見ているのか、それともオンライン to オンラインでできるのかというところをお聞かせいただきたい。

(デジタル庁澤田)

住民票に関しては、総務省でどのように進めていくか検討されているところで、我々の方からは回答できないところですが、この会議でフォーカスとしているところは、提示の場面については、スマホに入れたものを対面で提示する場面であったり、オンラインで提出を行う場面、オンライン経由で提出を行う場面、両方あり得ると考えております。

(笠井委員)

わかりました。それであれば、対面で提出する際の検証の機器みたいなところも、どのようにするのかという範疇の中で、あまりなかったもので、そのあたりもリスクに関係したりとか、利用者を絞るという観点では非常に重要な点かなということでございますので、一応質問させていただきました。

(國領座長)

はい、ありがとうございます。

(中村委員)

京都大学の中村でございます。皆様のご発言に関連する話ですけれども、細かく検討していくときに、リスクを分析するにあたって、利用シーンをどう分類していくかっていうところを、もうちょっと細かく考えていかないといけないかな、と思います。先ほどの富士榮委員からも、派生 VC がある場合とない場合というものを区別したりしたほうが良いのではないか、というコメントもありましたけれども、住民票の事例でも住民票に記載されている内容が正しいということが保証されていれば、別にそれを提示するのが誰かというのが関係ないというようなユースケースもありますし、確かに自分自身の住民票を持ってこれるところも含めて確認する、みたいなユースケースもあると思うので、VC が流れていって、他の人から提示されるというようなケースも想定するのか、明らかに本人が自身の VC として提示するということを検証するのか、というようなところがあるのかな、と。提示した VC も、提示した瞬間の有効性だけを確認すればいいのか、それを保存しておいて、ある程度時間が経ってから改めて有効かどうかというのを検証するようなユースケースもある

のか、とか、そういったところによって、リスクの分析の仕方とか、あるいは必要とする技術として、どこまで用意しておかないといけないんだってところが、変わってくるのかなと。

もう 1 点あるとすれば、証明書、例えば今の住民票としては、マイナンバーとか何も記載がないわけですが、デジタル化っていう意味では、個人に対する識別子をどうするか、だから DIW としてはどの識別子をどう扱うのか、とかも、議論の対象に入っていると思いますけれども、それを仮名化して紐付かないようにしないといけないようなユースケースもあれば、行政の手続としては、別に紐づいても良いというようなユースケースもあると思いますので、そこをどう分類するかみたいなところも考えないといけないかなと思います。その分類をした上で、今回はどれについて検討するのかっていうところが明確になると、技術を検討する上でも議論がしやすいかなと思います。

(國領座長)

他に、よろしいでしょうか。

(板倉委員)

弁護士の板倉です。どこにリスクがあるかっていうのは、誰に何を提示するかによって当然違うわけですが、Issuer への攻撃が危険な場合っていうのは、それを提示する Verifier の方が、それによって何らかの本人に対して、金銭的なダメージを与えるというのが多分一番リスクが高いのではないかなと思います。偽の Verifier というのが簡単にできるというのは、これはこれで別の話で、金銭的なというよりは、確実な情報が簡単に手に入るってことです。昨日もニュースでやっていましたけど、電車で偽の QR コードが貼ってあって、情報が抜かれるみたいなのがありましたが、Verifier に簡単に参入できるようになると、そういうことがより一層楽にできるわけで、その手当がいるのかなと思います。

これは去年も申し上げたかもしれませんが、悪い人たちは全く法律を無視して一番効率的に攻撃を考えますので、この文脈では一番緩い人に合わせて、一番緩い人をちゃんとやるように設計しないといけない、一番緩いもの同士でやられ放題やられたのが、某金融機関と某通信事業者の話ですから、そこを教訓にしてやらなきゃいけないっていうのがあります。

あとは、事業者の話色々お聞きしていくと思うのですが、事業者で属性確認なり本人確認なりをやるっていう際に、もちろん 1 つはそのコストが高いからやれない、という言い訳は、これは話を聞いて良いと思うのですね。今回のものはリスクを下げるという効果もあるわけですから。もう 1 つの種類として、本音を言うと変な利用者でも入ってきて欲しい、という人たちもいますので、はっきり言ってしまうと誰に売ろうが手数料が入ってくるわけですから、本人確認なんかろくにしないで、ショップに加えて手数料を取りたいプラットフォームというのがいるわけですよ。そういう人たちの話はもう最初から不当なものですから、不適切であって、要するに反映する必要はないという態度で臨まないと、事業者の話全部フラットに聞く必要はない、というところがあると思います。とりあえず、以上です。

(國領座長)

ありがとうございます。ご発言いただいたことを考えるにつけても、この会のゴールをどの辺に決定するかということも、もう少し明確にしてから進める方が良いと感じています。以前の会議体からですけれども、話題がどんどん広がっていくので、目指したいゴール感の事務局案を見せていただいて、その後で、じゃあそのゴール感が良いかということも議論した上で、そのゴール感に合わせて何を議論していくか、というような方針で、解像度を上げていけると良いかなど。毎年なかなか大変なのですが、よろしくお願いします。

(デジタル庁中川)

ありがとうございます。画面に出しております 34 ページの「議論のポイント」でございますが、まさしく、先ほどご議論いただきましたとおり、例えば、一度保存しておいてまた見せるといったユースケースなども、技術的には違うというような話もあります。ここをすべて包含してしまうと、最初に何から取り組みましょうか、というところになかなかたどり着けないとなりますので、まずはある程度取り付く島を作るという意味でも、ここから始めましょうか、というところからやっていくということも重要かなと思います。

その意味で、今ご議論いただいた内容、リスクの種類を一般的な形でありますけれども、させていただきまして、それにつきましてそれぞれの技術的運用、対策例みたいなものを右に示しております。「VC と Holder との紐づけ」であるとか、「Wallet 内のデータ管理」であるとか、「Unlinkability の確保」など、こちらにあげさせていただいているようなものですね。これを適切に技術面・運用面での対策を促すために必要な手法はどれか、そして先ほどおっしゃっていただいた意見のように、例えば住民票の写しを見せる時に、提出する人が、例えばその人であるということを示さなくても良いとか、そういうようなケースに絞って技術的・運用的対策例というのを考えた時に、仮にそうしたときに技術的に何をすべきなのか、その時にガイドラインとか、そういう運用面をどういうふうに縛れば、生きそうかというところ、こういうところを議論いただくというのが良いのかしら、と思っています。

次のページをお願いします。技術面、運用面の対策を主眼としていきつつも、個人の属性や資格を証明する公的かつリスクの高いユースケースと、デジタル庁でさせていただいている検討外でもあるというところもありますので、例えば公的に示すケースであり、また影響が大きいようなケースというのを、そこから取り付く島を作っていくというのはどうかと思っています。例えば住民票の写しというのは何度か出てきていますけど、結構クリティカルに確認をしなければいけないことがあるだろうか、というところを念頭に、ご議論いただきたいと思います。制度の縛りがなくても、「安価、簡便、迅速に」エコシステムが機能することになると、決めすぎることなくできるということで、役所が決めすぎることもなく、また技術的にも重いものをすることなくできればというところでございます。

議論のポイントは 37 ページで整理させていただきましたが、1-1、1-2、1-3、それぞれちょっとブレイクダウンさせていただいております。公的なユースケースを念頭に置くと、この推進に向けて

適切な技術面、運用面の対策を促すというのがあって、例としてガイドライン等と書いてございます。仮にそれがガイドラインであるのならば、どういう内容というふうなのを示して、作っていくということが大事なのではないかというところなんです。議論の時には、公的な VC を扱う Wallet の機能ですが、Issuer 適格性検証、Verifier 適格性検証というのを、それぞれの観点で作っていくことになると思いますので、このあたりを検討いただくということなのかと思います。この対象範囲や位置づけというのが、論点の 1-2 に出てくるのかなということ、そして、今回 1-3 に関しましては、そういう意味でこの検討会が行われたあと、技術ワーキンググループの方に移っていきますので、こちらで特に技術ワーキンググループで議論していただきたいこと、有り体に言えば宿題的な形で技術ワーキンググループに申し渡したいことがどういうことか、ということについて、ご議論をいただければ大変ありがたいかなと思います。

次のページもご紹介します。仮に、今年度ガイドラインを整備するとなるのであればということですが、骨子をまとめるということをやってみてはどうかと思っております。右側にガイドラインの目次というような形で書いておりますけれども、「はじめに」以下、基本的概念からリスク対策の推奨要件、参考情報等、この中でユースケースとしてこういうものをした時に、こういうリスク対策の推奨要件があるのではないかなというような、骨子を作っていただくということを、今年度のゴールにしてはどうかと思います。この中身については、そこから引き続きやっていくわけですが、こういうことをご議論いただきながらガイドラインで示すというのは 1 つの案かと思っております。事務局としては提示させていただいているところでございます。説明はこれ以上すると長くなってしまいますので、ある程度こういう形でさせていただきたいと思っておりますけれども、いかがでしょうか。このあたり、ご議論いただければ、よろしく願います。

(國領座長)

ありがとうございます。この辺のゴール感について、今映していただいているのが一番コンパクトにまとまっていると思うのですが、この辺のゴール感について、何かご意見ある方いらっしゃいますか。

中村先生は、いかがでしょうか。注文がちょっと漠然としすぎていて、もうちょっとはっきりしてとか、色々あるのではないかなと思うのですが。

(中村委員)

まとめ方、進め方としては、今ご説明いただいた形で議論を詰めていくということになるのかなと思っておりますけれども、具体的に言うと、今回の資料で 2 つユースケース提示いただいておりますけれども、いくつか場合に分けて、今回特に議論をしたいような詳細化されたユースケースが題材としてあると、それに基づいてそれぞれの観点、どこまで検討しないといけないか、どこまでリスクを考慮しないといけないか、というようなことが議論しやすいかと思っております。そういう意味では、ユースケースとしてどういうものを想定するのか、架空のものでも構わないとは思いますが、その共有がないと委員の皆様と意識を共有した議論がやりにくいかなと思います。そのあた

り時間かけていただけると、技術 WG に向けた準備ができるのかなと思っております。今の時点で具体的にどの観点か、とかまでは整理ができていないです。

(國領座長)

先ほど、場合分けをするべきじゃないかみたいな話があったのですが、この場合分けの場合の 카테고리 というのは、今の段階である程度イメージがつくのですかね。

(中村委員)

そういう意味では、もうちょっと詳細化した 카테고리 というか場合分け、こういう場合もあれば、シンプルにするためにはここはもう考えないことにする、仕組みとしては簡単に使っているようなことの観点が 5、6 個ぐらいは最低限出てきそうな気がしますので、そのあたりを整理した上でまずはその範囲で、それぞれの 카테고리 において、まずはそれぞれシンプルな状況においてどうか、というところを議論するのをスタートポイントにするというのが良いかなと思いました。

(國領座長)

ありがとうございます。手が挙がっているので、瀧委員お願いします。

(瀧委員)

ご説明をどうもありがとうございます。私からは 1 つ前ぐらいの、リスクの高いユースケースを念頭に、とあるところで、なんとなく思ったことをお伝えさせてください。

例えば高いリスクのもので、高い強度の下で手続を行っているとしても、本人が操作されているとか弱みを握られているとか、マニピュレートされているような状況を含めれば、決して最後まで、普通の人たちのリスク感覚として、リスクはゼロにはならないという側面が、投資詐欺とかだとよく起きることですけど、あると思っております。民間の事業者は基本的にリスクに対して、その発生確率と発生時の最大ダメージの掛け算のマトリックスを書いて、このリスクは取りませんとか、このリスクはあえて取りに行きますとか、バランスが悪いときは、それは対策をしに行きますみたいな判断をするので、高いリスクのところだけっていうところを平面的に捉えるというよりは、ダメージがコントロールできるのか、みたいな観点で見る必要があるのかなとは思いました。非常にリスクの低いケースもちゃんと 1 つ考えた方が良いのかなと思っています。適当な例を申し上げますと、例えば図書館で本を 5 冊まで借りられるようなクレデンシャルは何かというのは、最大の被害は本 5 冊みたいなところになると思います。図書館というのは割と緩めに、その辺の対応ができていますのかなとも思ったりしますので、グラデーションというか、最終的にはこの全体の枠組みとその現場の運用の中で、ダメージコントロールができていないか、という掛け算で運用がされることも多いのかなと思いますので、そういう観点が 1 つ、ライトなものも 1 つぐらいは見ておいた方が良いのかなと思いましたが、という意見でございます。以上です。

(國領座長)

ありがとうございます。横田委員、どうぞ。

(横田委員)

ありがとうございます。私もこの論点に関して申し上げたいことがありまして、前の会議で色々と議論をした時に、行政機関が受け取る場面についての法整備を進めないと、なかなか運用が拡大しないのではないかという議論がございました。特に民間発行のものを今回、射程に入れるかどうかによるのですが、昨今問題になっております、例えば卒業証書であるとか、そういう資格情報等、属性情報等きちんとつけて提供できるようにして、行政機関間での機関側での運用を促進するということにしないと、例えば、自治体と国の機関でのやり取りであるとか、あるいはその自治体における様々な AI エージェントの利活用において、資格情報の確認が非常に困難であるということが議論されているので、そこはかなりメリットがあるのではないかと。具体的に保育所等の優先関係を判断するのに AI を使って色々やるのに、その資格情報を目視で確認しているという例が、紹介されたところだと思います。ですので、今回適切な技術、運用面の対策を促す手法というところが議論になっているところですけども、基本的にガイドラインで行くということなのですが、このガイドラインの中にそのような受け入れの場の体制ないし、どういうものを受け入れるのかについての考え方というものが、含まれるかどうかについてお伺いしたい。また、法改正や、あるいは条例改正等が必要な分はやっていただかなきゃいけないことでもありますので、そのような議論を入れるかどうかについて、少し論点提供しておきたいと思います。以上です。

(デジタル庁中川)

ご意見ありがとうございます。法令の部分について、法律事項と我々は呼んでいますけれども、内閣法制局と折衝する時によく問われるのですが、これを定めなければいけない、もうそれしかないという状況までいくことによって、定めることができるということになっております。技術的な対策とか他の対策、さらに民間事業者の方の慣習であるとか、そういうものですに保護されているというものならば、そちらでやりなさいと言われることがあります。法律というのは、最低限で一番それしかない効果があるというので、そこをやっていくというのが主眼にどうしてもなってしまうので、そういう意味では、最初始めるとしても、一案ガイドラインであるのかなと思っているところでございます。

ご議論の中で思いましたけれども、17 ページのような住民票の写しの例があります。これは総務省とも協力しながら、お話をさせていただいていたりするのですが、よくあるユースケースというのはどういうものかという、いろんなユースケースございますけれども、世帯を全員示してこの家には誰がいて、補助金も申請するときに、市役所に、例えば世帯主が出しますというようなケースです。世帯主はマイナンバーカードみたいなもので属性証明以外にも自分の証明をするというようなケースを、まずもし何かするならば、そういうものを 1 つ考えた時に、周りの技術というのはどういうものが必要か、というのを考えてみるというのは、あるかもしれません。それを 1 つ柱に

した上で、例えば、じゃあ世帯主の証明はいらないというケースがあったとしたら、これとこれは抜けますね、みたいな形のガイドラインの大枠を作っていくっていうのも、一例あるのかな、と思いながら、お話を聞きました。

1 つテーマを作るとするならば、世帯主がその家族全員の住民票を持って補助金、児童手当みたいなものを申請するケースというのはどうでしょう。そういう柱を作りながら議論をしていって、いるもの、いないもの、みたいな形で議論はいかがでしょうか。

(横田委員)

この会議、公開になって初めての会議なのであえて申し上げますけれども、今のように選択的開示であるとか、あるいは証明をデジタルで完結させることというのが、市民にとっても受け取る行政にとっても、それを展開していく他の人たちにとっても、かなりメリットがあるということがわかるような形で議論を進めていただきたいと思います。そのためにも法改正や条例改正等が必要ならば、ためらわない方向で議論を進めるべきだと基本的には考えております。ただ、即座にそれが必要だと私も考えておりません。ただ中長期的にそのような議論の取っ掛かりとして、まずはガイドラインで適正なラインをきちんと示した上で、まずは使ってもらおう人たちが出てこないとうしようもないところがありますので、そういうものだと理解しております。以上です。

(デジタル庁中川)

横田先生ありがとうございます。まさしくおっしゃるとおりで、1 つ何かを考えたときに、やはり法律が必要だということになれば、政省令であったり、法律であったりというのは、もちろんできるということだと思います。まずは、そういう意味で何かしらのユースケースにして考えるということから始めていきたいと思っております。ご意見ありがとうございます。

(松本委員)

横田委員の話で中長期的という話があったけれども、そこも私が懸念している点の1つで、ここで行っている趣旨はよくわかるんです。なるべく法律の改正とかなしにできることをやって、それがみんなに受け入れられるのをまずは立ててあげたいという趣旨はよくわかるのだけれども、それはCan-Beですよ。To-Beについて何も考えずにCan-Beをやるのは結構危険だなと思っているところがあって、やっぱりTo-BeはTo-Beでみんなこっちの方向に行くよねっていうのは指し示す必要があるんじゃない、というのが、そこは議論しないんですかっていうのは少し疑問があります。極論から言えば、最終的には2005年のe文書法みたいに一括法で資格はすべてVCを使わなきゃいけないっていう強制力を働かすような法律があっても良いのではないかというふうに思っているところがあって、2005年のe文書法は民間で保管が義務付けられた文書の電子化容認の一括法で、紙文書から電子文書へは推進したのですが、それだけではマシンリーダブルなデジタル文書の推進にはならず、結果、紙文書と同様で人の目視でしか確認できない。その次に行くためには、自動的に処理できるようにしなきゃいけないわけであって、そういうのがTo-Beとしてあって良い

んじゃないかなと考えていくわけです。ここの議論じゃないのかもしれないですけどね。

(國領座長)

ありがとうございます。富士榮委員はさっき手が上がったのが残っているのか、それとも改めてでしょうか。

(富士榮委員)

改めて挙げたものです。

(國領座長)

わかりました。じゃあ言ってください。その後、松尾委員をかなり待たせているような感じがするので、順にお願いします。

(富士榮委員)

手短に 1 つだけです。ガイドラインをゴールとするということについては良いと思っていますが、ガイドラインに Verifier なり Issuer なりがちゃんと遵守して運用されているってことが、利用者にとってわかるようにしなきゃいけないだろうっていう話が 1 つ感じたところです。特に、AI エージェントの話もありましたけれども、定性的に人が感じる以外に、機械的にそういうものが判断できるような状態っていうのを作っていかないと、いわゆるノンヒューマンアイデンティティと言われている世界においては、ワークしないようなものになってしまうのではないかなとも思いますので、技術ワーキンググループの方で考えることかもしれませんが、そういうところまで踏み込んでガイドラインというのを作って、それを強制していける仕組みと併せて展開できていくようにゴール感を精緻化していただけると良いかなと思いました。以上です。

(國領座長)

ありがとうございます。松尾委員、お待たせしましたどうぞ。

(松尾委員)

ありがとうございます。ただ、質問は横田委員以降で出たことを質問したかったので、重複するのですが、そもそもガイドラインを作るに当たってどうやって強制をするかというか、皆さんに使っていただくのかっていう道筋がとても大事で、もうすでに皆さんおっしゃっていただいたので、ほとんど付け加えることはないのですが、例えば誰が実装するかによって、国が実装するのか、ローカルガバメントが実装するのか、民間が実装するのか、パブリックセクターのユースケースもあれば、民間ユースケースもあれば、官民のユースケースもあるという中で言うと、それぞれ異なる実装主体がある中で、それぞれの目線が揃っていないと、連携が前提になる中で認識が違ったものが実装されていくと、将来のいさかいの種になることは、完全に見えている話です。そ

の意味で、このガイドラインが例えば国レベルのパブリックセクターなのか、ローカルガバメントなのか民間なのか、どういうふうにご活用いただけるのか、それが例えば調達基準に入るのか、というところを、ある程度見越した上で書きぶりを作っていく、あるいは、普及のさせ方で、一気に法律作ってというのは当然美しい姿であるものの、そうするととても時間がかかるので、そうじゃないとしたとしても、このガイドラインがどういう風に受け取ってもらえるのかっていうのは、よくよく考えた上でガイドラインを出していく必要があるのではないかなと思った次第です。以上です。

(國領座長)

ありがとうございます。笠井委員、お願いします。

(笠井委員)

ありがとうございます。私も先ほどの法制度の縛りがなくとも、エコシステムが機能するのが望ましいというところが、どうしても疑問でございまして、公的ならいいのですけれども、前回の検討会でも伝えましたが、民間が頑張って普及しようとすればするほど、次に独禁法の観点が来ますよねということで、コンビニはどうしても寡占状態ですので、気になる点でございます。そういう観点で言うと、もちろん取り扱わないガイドラインみたいなところもゴールでしょうし、どうしても法制度を作った方が普及しやすいという観点とかも出てくると思われるので、縛りがなくとも機能することが望ましいが、どういうフェーズになった時に法制度が必要なのかということについても、民間と公的の違いだと思いますけれども、民間においてもそういうことが出てくるという観点はコメントさせていただきます。

(國領座長)

ありがとうございます。笠井委員のところは、結構具体的な選択的屬性開示をしたいという、差し迫ってという大変ですけども、大臣が2年ぐらい前にデモンストレーションしたやつを、まだできてないのかという話ですよ。

(笠井委員)

そうですね。読み取る側、どちらかというとVCなりなんなり本人確認をしたい読み取る側で、お酒・タバコを検討しておりますが、読み取るルールをコンビニ各社一緒に大丈夫でしたっけ、とかですね、現実的に事業を考えた時には課題になるものでして、公的であれば良いと思うのですけれども、民間で結局普及させたいとなった時に、寡占でとかになった時には、やっぱりそこに出てきてしまうので、場合によっては認定制度とかそういうようなものが必要かなと思っております。

(國領座長)

ありがとうございます。それぐらいの具体的なイメージがあると考えやすいですね。板倉委員、お願いします。

(板倉委員)

弁護士なので法律がないと仕事にならないからというわけではないですが、既に挙げていただいたリスクの中でも、公的なところが発行するとしても Wallet は出てくるわけで、その Wallet が永続的かっていう話はあるわけでありまして。これはデータポータビリティの話になりますけど、データポータビリティは令和に入ってからだったか、ちょっとその前ぐらいだったかに議論して、個人情報保護法にも微妙にそれっぽいものが入ってはいるのですが、ベースが電子でも、紙で出さないとなっていたところを、できれば電子で本人に開示してあげてくださいね、という非常に中途半端な形でしか入っていませんので、日本ではデータポータビリティ権みたいなものはありませんし、だいたい問題になる時というのは、すでに法的整理の手续が走る場合がありますので、そうすると、裁判所の管財の話になっているので、これは法律がないとガイドラインでどうにかできるって話でもありませんから、ここはやるとすれば、もう1回データポータビリティに向き合わざるを得ないというのがあります。

もう1つは、先ほど笠井委員がおっしゃった独禁法との関係なのですが、サプライチェーンにセキュリティを強要するということすら、横のカルテルの話ではなく、優越的地位の濫用の関係で問題があって、公正取引委員会がガイドラインっぽいものを出しているのですが、先ほど申し上げたように、この仕組みは最低線の底上げをしないといけない話ですので、みんな守ってもらえないといけませんから、そこは完全に法律作るかどうかはともかく、少なくとも優越的地位の濫用にならんよ、とサプライチェーンのセキュリティはまとめて確保されないといかんよ、ということになりますので、何らかの独禁法違反にならないような仕組みがいるというところはとりあえず指摘しておきます。以上です。

(國領座長)

崎村委員、お願いします。

(崎村委員)

ありがとうございます。かなり皆さんおっしゃっていただいたので、重複するところはあるのですが、やはり軽いユースケースをやるべきだと思うのですよね。EU Digital Identity Wallet でも、だから年齢認証から始めると。今軽くやっているところなのですが、その辺からやっているというのがありますし、子供のほうの観点からも、国際的に見ても今非常に年齢認証というか、年齢電子認証というのか、その部分は選択的開示でちゃんとやっていくということが、非常に真剣に議論されている、国際基準も出るという状態になってきているので、そういったことはやっぱり考えていきたいなと思う。

あと、Wallet の認証が結構問題で、選択的開示ができるって言っても、結局本人に対して十分でかつ簡潔でわかりやすい形で、なぜその情報が必要なのかというのを示すことができないと、選択的開示の意味が全くないのですよね。それから、情報提供先、Relying Party が要求するもの

が適切なのか、というデータミニマイゼーションがちゃんと効いているのかというのも、ユーザーはほとんど判断できないですよ。なので、その辺をどうするのかというのは、今、まさに Internet Identity Workshop というのに来ていますけど、その辺盛んに議論されているところなので、そういったこの観点というのはある程度ガイドラインを考えるにしても、考えていった方が良いのではないのかなと。制度としてはあまりうまくいきませんでしたけど、情報銀行の認定制度で、要求していることの表示の仕方だとか、そういったところかなり入っているので、ああいうのも参考にしながら進めていくのが良いのかなという感想を持ちました。以上です。

(國領座長)

ありがとうございます。ここで、本日欠席されている若江委員から事前に意見をいただいているということだと思うので、事務局から紹介いただけますか。

(デジタル庁澤田)

若江委員からいただいた意見を、ここで読み上げさせていただきます。

「ハードローによる規制(遵守しない場合に制裁がある共同規制を含む)を検討対象から外すべきではないのではないか。「国のルールや制度は存在せずとも上手くエコシステムが回ることが理想」という点は、もちろん、それが上手く回ればいいが、ルール不在の状態では、悪用されて消費者被害やプライバシー侵害が発生するおそれもある。不信が広がれば普及しなくなるかもしれないし、逆に、大手で安心感のあるグーグルやアップルの Wallet に利用が集中し、寡占を進めるかもしれない。それは「プラットフォームの手にあったデータのコントロールを取り戻す」という DIW の目指す姿とは異なるはず。

民間または公的な認証制度が機能すれば、それが一番だが、認証制度が機能するのは、消費者に安心・安全なものを選びたいという要望がある場合に限られる。情報銀行の例でも分かるように、目に見えないデータのリスクに関するサービスは認証制度が機能しにくいとの指摘もある。まして DIW のように便利な反面、難解な技術によって支えられるサービスの場合、消費者はどこにリスクがあるのか分からないため、認証の有無を気にしない場合もあり、ベンダーに認証取得のインセンティブは生じないのではないか。

既存の法律での対応も提案されているが、少なくとも個人情報保護法で DIW のプライバシーリスクに対応することは難しい。例えば、選択的開示による取得データの最小化やトラッキング防止を実現するためには、ゼロ知識証明の採用や、署名値のランダム発行などの措置を講じてもらうことが重要だが、個人情報法はそれを遵守させるための法的根拠をもたない。GDPR のデータ最小化の原則は「目的達成のために必要最小限しか取り扱ってはいけない」という厳格なもので、酒を売るなら 20 歳以上か未満かのデータしか取得できない。しかし、日本の個人情報法の場合、利用目的を特定し、通知公表さえすれば、多種多様な目的(本来の目的とは全く関係ないものを含む)を設定してもその目的で取り扱うことが可能になる。本人の同意も不要である。さらに、個人情報法の利用目的の制限や適正取得義務などの規律が対象としているのは「個人情報」で、DIW で検証者が取得

する情報は必ずしも個人情報にはあたらないことも多い。「個人関連情報」に該当したとしても、個人関連情報に対する同法の規制は、それが第三者提供により個人情報に変わった場合の同意取得のみである。

Wallet Provider には多くの情報が集積することになるが、現状では Wallet Provider が利用規約等で利用目的を特定していれば、本来の利用目的とはまったく関係のない目的に利用することも可能。仮に、今後、グーグルやアップルの寡占が発生し、選択肢が減り、しかも DIW を利用しないと様々なデジタルサービスを受けられない状態が生じた場合、本来の目的とは異なる一定の用途への利用を禁じる必要もでてこないか。

検討対象のユースケースについては、行政が証明書を受け取るケースを想定する場合、検証者の悪用がイメージしにくくなり、幅広リスクを検証する上で適当ではないのではないかと。今後の利活用拡大を見据えて幅広いユースケースを対象範囲とするべき。

なお、冒頭の『「安価・簡便・迅速に実施できること』が重要』という設定には違和感がある。DIW が世界で注目されているのは「ユーザー中心のデジタル ID 管理」、つまり、これまでプラットフォームの手にあったデータのコントロールを取り戻せるという期待のほずで、それができないのに「安価・簡便・迅速」に利用できても本末転倒。その意味でユーザーの権利や利益の保護が重要で、「安価・簡便・迅速」に「安全」を加えるべき。」

以上であります。少々長いものを時間の都合で早口で読み上げいたしましたので、簡単にまとめますと、主に Wallet Provider の観点で何らかの手法が必要ではないか、また、一定の安全を確保するために「安価、簡便、迅速なものが」という点についての疑問提起をいただいた、というふうに受け止めております。事務局から欠席者の若江委員のご意見のご紹介をさせていただきました。

(國領座長)

ありがとうございます。これで、ご発言の要求は一応カバーされたということだと思います。今日いただいたゴールイメージに関連して皆さんの意見を総括するのはとても大変なのですが、ユースケースとか局面によって、使われ方には色々バリエーションがありそうで、すべてのバリエーションのすべてのリスクを掲げて、それに全部に対応するという考え方っていうのは大変で、ガチガチになってしまう。このユースケースは利便性が非常に高いところとか、リスクが非常に高いところとか、使われ方のパターン別ぐらいに分けて、その分野におけるガイドラインの作り方みたいなことについて議論していくと、何が変数なのかというのを整理した上で、その使われ方におけるリスクというのがどんなリスクみたいなことがあって、それに適切に対応するためには、どんなガイドラインが必要なのかというようなことを考えていくのかなと。

その中で住民票を使いながら、年齢確認の選択的開示していくユースケースは、かなり見えているところがあるので、そういうところは具体的に考えていきたい。どう考えても、今年で網羅的なガイドラインが網羅的に書けるとはとても思いがたいので、一体どの辺が全体像なのかというざっくりしたマップと、その中で利便性高くて、これくらいのリスクのものやつは早めに動かしちゃった方がよいのではないかとと思うような分野にフォーカスしながら、そのリスクについてどう考えるべ

きか、受け取る人、いろんなプレイヤーがいるわけですが、Verifier がいたり、Issuer がいたり、Relying Party がいたり、それぞれのパーティーに対して、どのような義務付けをした方が良いのかとか、ガイドラインだけじゃなくて認証みたいなこともした方がいいのか、というようなことでしたかね。その辺も議論に含めて、具体的なイメージを作っていくって、とにかく今年作ってみるといような感じが、ざっくり流れだったような気がしたのですが、どうでしょう。

(笠井委員)

ありがとうございます。これをまとめるのは非常に難しいのかなと思いつつも、何か公表されるガイドライン等を私どもを使う側としては、普及をどういうふうに、といった時に、まだ VC とかデジタル証明といっても、社内の中でも理解が得にくいところがあります。ですので、何かしらガイドブック、ガイドラインなりが出たと同時に、そこで頑張ってる事業者を引き出して、イベントではないですけども、普及活動みたいなところも、ぜひ利用者側としてもお願いしたいです。そういう流れの中で先ほど言いましたけど、機器みたいな話も出てくるものでして、ちゃんとプレイヤーが出揃った検討をなされるべきと思っておりますので、盛り上げというか、利用シーンの盛り上げみたいなところは、私ども消費者側に近い人間とはお願いしたいところかなと思っております。

(板倉委員)

松本委員言っていたことは、「はじめに」の 1-1 には私は書いた方が良く思っていて、デジタル庁自体の存在意義がデジタルファーストですから、究極的にはこれをやる以上は、紙はなくしてこれにしていくんだ、というのはあっていいのではないかなと思う。

もう一つ、出てこなかったのと言うと、住民票のデジタル化を総務省がやられるということですが、ただ住民票の取得を eKYC でやるというのは裁判で争われた話でありまして、ダメだとしたわけですね(東京地判令和 4 年 12 月 8 日判時 2608 号 27 頁)。しかも裁判中に省令まで改正してダメだとしたわけです。凄いことやるな、と思いましたが、後から見れば eKYC はどんどん攻撃されて、いまやマネロンの関係でもうやめようという話になっていますから、結果的には適切なのですが、とすると、それはダメだというぐらいのレベルの確実性を持って、住民票の情報というのは使ってほしい、というのが根底にはあると思います。取得の段階ですら相当の本人確認をしないと取得できないという情報です。なぜか郵送は良いという、そこは、私は最後まで読んでよく納得できないのですが、でもそれぐらいのレベル感でやられているという前提でいくわけですから(安易な流通は認められないでしょう)。口ずっぱく言っていますけど、とにかく悪い人というのは、一番儲かるところに全勢力を、法律を無視して、投下してみんなを攻撃しているわけです。その結果、カンボジアの国境のところで悪い人たちが、捕まっている日本人がいるとかなっているわけで、本当に敵は世界的なマフィアであって、どこがどうやって儲かるかっていうのさえわかれば、ただ全力でそこに投入してくるわけです。最低線が安全なように設計しないといけないというわけでありまして、かつデジタルファーストにしないといけない。人は減るし、コストは上がるし、もうそうしてい

ないとみんなもたないわけです。マイナンバーカードはものすごいやり方で無理やり普及させた結果、公的個人認証がいろんなところでなんとか使えるようになっていまして、閾値がある一定を超えると普及するんだというのがあります。もちろん先ほど笠井委員がおっしゃったように、機器はどうするんだっていうのはありますが、それはソフトウェアで解決できるのであれば、みんなのところにスマホはありますので、そっちの方向も見据えながらやっていくのかなと思いますが、この 1-1 のところにデジタルファースト、僕は究極目標だよと、来年やれとは言いませんけど、いうのは書いた方がいいのではないかなと思っています。はい、以上です。

(國領座長)

ありがとうございます。他にいかがでしょうか。

(松本委員)

ユースケースは重要だと思うのですよね。ユースケースによって関係するステークホルダーが変わるので、ある意味でユースケース関係の対応的なことも、考えないといけないことがいっぱいある。その中で住民票というのは、私的にはあまり関心がないというか、そもそも住民票いるの、というのが私の疑問で、要はマイナンバーカードで自分の証明ができますので、あとは世帯情報なのだけでも、これが今の法律ではできないけれども、マイナンバーで、連携基盤で自分の意思によってこの企業にプッシュしてほしいというのはできるべきだと思っているのですよね、マイナンバー法で。それで解決するのではないかと昔から思っていて、それがバックオフィス連携ですよ。フロント連携が VC のやり方なのだけど、どっちがいいかはわかんないですよ、今の段階では。それを含めて、私は、目指すべきはもっと民間、民民の間であるとか、そういうのが、本来目指す姿じゃないかなというふうに感じます。話、戻りますけども、今できることをやるっていうのと、将来どうなるかっていうのはやっぱり両方考えないといけない。

(國領座長)

ありがとうございます。ゆくゆくは民民で使う公的な証明みたいなものも、当然視野に入っているわけですよ。むしろ、そっちからやったほうがいいぐらいだ、とおっしゃっている。

(松本委員)

勘所はそこではない。ゴールというのは議論していないし、そこはみんな考え方が違う。

(國領座長)

逆に官官の間のやりとりぐらいだと、バックエンド連携の方が良いのではないかと。

(松本委員)

そのとおり、それは前回も言った。Once-Only Principle はまさにそういうこと。欧州では Once-

Only Principle ってありますよね。あれはまさに、行政機関自体では、こういった住民票のやり取りをフロントではやらないはずなので、もともとの思想としては。VC でやった方がほうが良いケースも、今はあるかもしれない、実際には、ただ、それがゴールかどうかはわからない。

(國領座長)

やはり具体的なユースケースをいくつか念頭に入れて、検討していただくようなことになるのでしょうね。その時に、官官の話と、民民に公的な証明書を使ってみたいなのは、タバコを買うのに年齢確認というのは、あれは民民ですよ。

(デジタル庁楠)

法令に基づく年齢確認なので、民が官から課された義務を遂行するための民民のユースケース。

(國領座長)

そっちの方がなんか大きいんじゃないかって。個人的には私もその感覚が結構あって。

(デジタル庁楠)

私もそこは全く同感で、ここは明らかに情報提供ネットワークシステムでカバーできないところなので、大きく期待しているところではありました。

ただ、なんで官を主語にしているか、というのも、多少の理由はありまして、やっぱり自分ごとにしなとなかなかできない、特に住民票というのは歴史的にも本人確認書類に準ずるものとして使われてきたからこそ、あれができちゃいけない、これができちゃいけないという、かなり厳しい要件が、今回総務省の検討会でも議論が出てきたので、ある程度厳しいものでどうやればできるかというのを含めて言うと、それは、民民のユースケース、例えば成績証明書であったり、会社の在籍証明書であったり。あるいは、転職時、私はデジタル庁に入るとき何枚エクセル用紙を書かされているんだろうと、本当にデジタル敗戦をかみしめながら入庁したので、なくしたいのですが、毎年現況報告とか、おおよそ普通の人々が正しく書けると思えない、だいたい所得と収入の区別がついている日本人って何人、何割ぐらいいるんだろうと思いつつ、あれを年末調整のためにちゃんと書かせている総務部って本当にすごいな、と思うんですけども、おっしゃるように、最後、これ民民に援用していくところを大きな射程に入れているんですけど、我々が自分ごととして受け止めていかないと説得力がないという意味で、官民、官官のシナリオを含めているということで、おっしゃるとおりだと思います。

(國領座長)

この場合も、官が発行する VC の話と官が受け入れる VC の話とがあって、官が受け入れてもいいと思うぐらいの VC というのはやっぱりレベル感が高くなって、そこぐらいに合わせておくと、汎

用的なものにでも堪えるではないか。それを基準にしちゃうと厳しすぎちゃって、使い物にならないということも考えたいですね。

(デジタル庁楠)

本音で言えば、できれば民間も真似したくなるぐらい軽いもので、それを実現していくというところをどこまでできるかというのが望ましいです。2年ほど前に処分通知等のデジタル化の時には、要件を言語化していった、できるだけコストが小さくて平易な実現方法が実はたくさんあって、デジタル署名だけではない、みたいなのを詰めていったのですけれども、要件は高めに設定した上で特殊なインフラで国にしかできないような方法でやるのではなく、それこそレシートの発行ひとつとっても誰でも簡単にできるような方法で、この要件を満たすっていうところまでできればな、という期待をしています。

(國領座長)

ありがとうございます。これぐらいで、中村先生できますか。

(中村委員)

雰囲気は。もう少し素材があれば。

(國領座長)

どんな素材が欲しいでしょうか、やはりユースケースでしょうか。

(中村委員)

そうですね、ユースケースが欲しいです。また、先ほど卒業証明書の話も例として出ましたけれど、現時点の卒業証明書の確認、あるいは卒業証書の確認みたいな、作れちゃうけど信じましょうみたいなレベルで、それをデジタル化するっていうところを考えるとスタートポイントにするのか、デジタル化する以上は、それなりに信頼性のあるものを作りたいねっていうところを目指すのかが、デジタル化する以上は、方向性としてあって、いきなりみんな署名を打ちましようとか、そういう信頼性の高いものを作ろうと思うと、制度としてしないとだめですよっていうような裏付けがないと、世の中の動機には動きにくいのかなっていうところもあり、VC・DIWというのを思考実験的に議論する方向でとどまる結果になってもいいのか、将来的に世の中で役に立つものを目指して、みんなで議論しましょうという方向でいくのかが、ある程度意識合わせをしておいて議論したいなと思いました。

(國領座長)

やっぱり最後は使いたいねっていうふうになりますよね。

(デジタル庁楠)

紙は結構いい加減なのですよ。デジタルにした時に同じようないい加減さで受け入れられるか悩ましいところで、紙よりもコピーが簡単だとか、書き換えるのも簡単だから、もうちょっと高いレベルを求めたいとなるのではないかと、いう気もします。

一方で、我々電子署名法、電子委任状法等を所掌している中で、厳し過ぎてもなかなか普及しないというのを、この e-Japan の四半世紀の中で見てきているから、もうちょっと軽くなれないか、紙と同じでいいとは思わないけれども軽くなれないか、例えばイメージ的にはよし悪しはあるけれども、SSL って普及しましたと、銀行の取引とか結構センシティブなユースケースだと思うのですが、ちゃんと使われています。フィッシングとかいろいろ問題はありますけど。

コマースに関しては、これから AI エージェントのためのいろんな基盤となるプロトコル、今日ご紹介あったと思いますけれども、A2A なり、Agent Payment Protocol みたいなものを見ても、プロトコルレベルで電子署名技術が入ってきて、証跡をきちっと残すという世界になっています。ここの責任分界点は、将来、法律事項が出てこないとも限らないですが、民法の証拠力の世界を詰めていって、解釈だけでいける部分も相当あるだろうという気もします。解釈とか現行法の運用だけでクリアできない部分が、もしここで明らかになるのであれば、そこはしっかりと背負っていくきっかけにはなるのかなと思います。要件を明確にしていき、何が望まれているかを整理して脇を締めておくことによって、社会の混乱を招かないか、をご議論いただいた上で、できれば特別なことをやったり、少数の人しか使えない仕組みではなくて、等しく住民の方々が使うことができ、日本だけではなく世界で、こんなやり方でいいよねとなっていく、ある種、普遍性なり無理なく普及できるような着地の中で、紙をなくすような仕組みというのができていけば、一番ありがたいなと思っています。

(デジタル庁中川)

ご議論いただきまして、やはり民間にも広がりを持たせるユースケースというのはあっても良いと思いますので、仮ですけれども、例えば住民票を、先ほど笠井委員もおっしゃっていたように、民間が受け取った時、例えば携帯電話事業者が本人確認書類として受け取った時に、受け取った時のデバイスってどういうものであるだろうか、どういうふうなユースケースであるだろうか、ということで、官から発行したものを民が受け取った時というのを 1 回柱にしてみて、民への広がりを見てみるというのはいかがでしょうか。

(デジタル庁楠)

役所が受け取る、民の書類を受け取っているといえますか、確定申告の時には領収書が入ってきますし、民と官、官と民というのは非常に多いので、この辺で、典型的で紙が多く残っているものというのは色々出てくると思うので、ユースケースを広く、次回までにはわからないかもしれませんが、議論を深めていくのが良いかなと思います。デジタル化した割には、全然紙がなくなっていないので、具体的なユースケースをご意見いただきながら、整理していけると良いのかなと。

たまたま住民票に関しては、まさに総務省の検討会で我々に今バトンを渡されているところなの

で、ここは 1 つしっかりと整理をする必要があるのですけれども、行政手続に限っても民と官をまたいだ紙というのは他にも多くありますし、民の転職 1 つとっても、紙の束で大変なことになっているので、打ち取れるもの、打ち取れないもの出てくるかもしれませんが、前広にご意見いただきながら考えてけると良いかなと思います。できるだけ困っている、どうしようもないやつをテーブルに乗せられると良いと思います。

(國領座長)

それでは、想定どおり色々なのですけれども、ただ、その中でも何を議論しなければいけないか、どの辺狙わなきゃいけないかということについては、皆さんの共通認識できたと思いますので、その中から、最後、発注者責任で、これでやってよ、この議論を受けてイメージいただけると、その枠の中で具体化すると一体どういうイメージになるのか、どういうガイドラインが想定できるのか、後でそれがもう 1 回汎用性があるかというのは検証しないといけなくなると思うのですけれども、まずはどういうパターンがあるかのマップの中から、ここがニーズがすごく高い、だからここでやってよ、というのを発注者責任で言っていたと議論が進みやすくなるような気がしたので、よろしくをお願いします。

それでは事務局にお返して良いですか。

(デジタル庁北井上)

ありがとうございました。

閉会に先立ちまして事務局から事務連絡をさせていただきます。本日いただいたご意見、今、座長におまとめいただいた点も当然含めまして、次回以降の議題ですとか、あるいは技術ワーキンググループでの議論というところに反映をして参ります。また、本日の議事録については後日、委員の皆様にご確認をいただいた上で、デジタル庁ウェブサイトにて公表させていただきます。また、次回会合や技術ワーキンググループの開催につきましては、資料 3、今投影しているものでございますけれども、こちらに記載のとおり予定をしております。具体の説明は、時間もやや過ぎておりますので割愛いたしますけれども、関係委員の皆様におかれましては、引き続きどうぞよろしくをお願いいたします。

事務連絡としては以上となります。それでは本会議の閉会にあたりまして、事務局を代表いたしまして、デジタル庁デジタル社会共通機能グループ長、楠よりご挨拶を申し上げます。

(デジタル庁楠)

本当に皆様、闊達にご議論いただきまして、ありがとうございます。

今日すごく楽しみにしていたのですが、日取りがたまたま大臣着任の翌日ということで、終わりだけの参加になってしまいました。後で議事録含めしっかりと拝見させていただければと考えております。

今日いただいたご意見を、しっかりと技術ワーキンググループに引き継いで、この VC や Wallet

に求めている具体的な技術的要件というのを詰めていくことになる、その後、改めてこの本体会議を開会できればと考えております。

昨年、一昨年の議論を振り返ると、e-Japan の始まりの頃には、ダウンロードしてアップロードしてみたいな操作がパソコン、ブラウザでは簡単にできていたのが、スマホになってタッチUIの中でどうやっていくか、というところで、束ねて提示するということが急に難しくなってしまうと、この辺を Wallet でしっかりやっていかなければならないよね、と、そして Wallet に入れていく紙は本物か検証できないといけないから、VC とか mdoc とか今出てきている技術を押さえながら、どうやって紙をなくしていくために使えるか、みたいな議論がありました。

また、マイナワーキング以来、本来公共サービスメッシュでバックオフィス連携をやろうと思っていた色々なことが、制度上の壁もあって、本人を介した情報連携とか何か別のやり方をやらない限り、例えば情報提供ネットワークシステムには 4 情報を流すこともできませんし、あるいは符号変換の仕組みが入った瞬間、戸籍や住民票のように複数人についての関係を示すところが、プライバシーを保護していて、円滑にやっていくという仕組みがない。松本委員から、本当はバックオフィス連携でやるべきなのか、フロントでやるべきなのかという課題提起はありますけれども、これはまさに、2020 年ごろに議論をしていた時には、漠然とバックオフィス連携でやろうとしていたことが、デジタル庁もこの数年の歴史の中で、ほぼほぼちゃんとできなかった。そのための制度改正に、いろいろな壁にぶつかっていくし、併せてバックオフィス連携でできるのは所詮、官官のやりとりだけで、手続における紙というのは民が入ってきて、民官、官民ってすごくたくさんありますので、アップフローでどうやって変えていくかということのためには、フロントも含めた仕組みが必要だということの認識を新たにしたところでもございます。

今年で言うと、ちょうどオープン AI が Atlas を発表して、その前に Perplexity のコメントを出しているなど、今年は一エージェントブラウザ元年になると思います。これは結構怖い話だと思っていて、ブラウザには自分のいろんなクレデンシャルが溜まっていて、それを全部 AI が代わりに叩くことができる、ある種人類が AI に軒先を渡した年に今年はなっているわけですが、おそらく、自分についての住民票とかいろんなものをエージェントブラウザがワンストップで手続をするために、みんな預かるということが普通になっていく。来年の確定申告を AI ブラウザでやる人が出てきてしまう、これはもう現実としてですね。いろんな事故が起こるのではないかなと思うので、それを畳みにいくではないですが、これから起こるであろうことを少し先回りしながら、ある程度安全に AI エージェントにいろんなタスクを任せていく、ここのプロセスの中に偽の文書とかが入ってこないようにしているというのは、ますます重要になっているということで、いわゆるスマホの Wallet だけではなく、ここでご議論いただくことというのは、これからの 10 年、20 年、人類がちゃんと AI を乗りこなすためにもとても重要な議論だと思いますので、ぜひ具体的なアウトプットを出して、あの時ちゃんと議論してよかったなというところまで持っていければ一番良いと思っております。ぜひ委員の皆様には、引き続きご支援いただければというふうに思います。よろしくお願ひします。

(デジタル庁北井上)

ありがとうございました。それでは以上をもちまして、「属性証明の課題整理に関する有識者会議」第1回を終了いたします。ありがとうございました。

以上